Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (cancelled)

Claim 2. (currently amended) A tamper resistant processor system, comprising:

a multi-component chip module (MCM) including:

a single CPU;

one or more memory chips;

one or more chip means containing at least one each of a de-encryption key and algorithm therein;

an obscurant covering the contents of said multi-component chip module;

further comprising said multi-component chip module in a bus configuration with other multi-component chip modules and said one or more memory chips;

further comprising a memory clear feature; and

further comprising de-encryption key and algorithm self-destruct feature.

Claim 3. (currently amended) A tamper resistant processor system, comprising:

processor boards;

processing chip;

an encrypted computer program;

a non-volatile memory, operatively connected to said processor boards, for storing said encrypted computer program and sending said encrypted computer programs to address destinations on said processor boards;

multi-component chip modules for receiving and de-encrypting said encrypted computer program and sending said de-encrypted computer programs to memory components on said multi-component chip modules;

wherein said computer program requires no token to activate or authorize use; and

wherein said computer program is loaded onto a chip.

Claim 4. (currently amended) A method for protecting a processor system from tampering, said method comprising the steps of:

a) mounting IC components on a single substrate as a multi-component module or as the contents of a multi-component module;

b) converting an encrypted computer program, received over a bus from a non-volatile memory, into its original un-encrypted form;

c) sending the de-encrypted computer program to appropriate locations in memory located in the multi-component module;

d) protecting the multi-component module using one or a combination of an obscurant, deceptive patterns, and tamper detection/destruction mechanisms; and

e) wherein said deceptive pattern comprises decoy mounted IC components.

Claim 5. (currently amended) A tamper resistant processor system, comprising:

processor boards;

encrypted code;

a non-volatile memory, operatively connected to said processor boards, for storing said encrypted code and sending said encrypted code to address destinations on said processor boards;

multi-component chip modules for receiving and de-encrypting said encrypted code and sending said de-encrypted code to memory components on said multi-chip modules; and

further comprising controls for user authorization at multiple security levels.

Claim 6 (cancelled)

Claim 7. (currently amended) A tamper resistant processor system, comprising:

processor boards;

encrypted data;

a non-volatile memory or network data source, operatively connected to said processor boards, for storing said encrypted data and sending said encrypted data to address destinations on said processor boards and for receiving and storing encrypted data resulting from the processing of the input data;

multi-component chip modules for receiving and de-encrypting said encrypted data, sending said de-encrypted data to memory components on said multi-chip modules, for storing the results of

processing the de-encrypted data, and for encrypting the results before sending to storage or network external to the multi-component chip modules; and

further comprising controls for user authorization at multiple security levels.

Claim 8. (currently amended) A method for protecting a processor system from tampering, said method comprising the steps of:

a) mounting IC components on a single substrate as a multi-component module or as the contents of a multi-component module;

b) converting encrypted data, received over a bus from a non-volatile memory, into its original unencrypted form;

c) sending the de-encrypted data to appropriate locations in memory located in the multi-component module;

d) encrypting processing result data that is being sent to storage or networks external to the multi-component module; and

e) protecting the multi-component module using one or a combination of an obscurant, deceptive patterns, and tamper detection/destruction mechanisms; and

f) wherein said deceptive pattern comprises decoy mounted IC components.

Claim 9. (currently amended) A tamper resistant processor system, comprising:

a multi-component chip module including:

a single CPU;

an in-line real time de-encryption chip;

one or more memory chips, operatively connected to said in-line real time de-encryption chip, said multi-component chip module encrypting out put to said one or more memory chips;

a memory controller selecting between secured and un-secured memory over a processor bus; and

said de-encryption chip allows multilevel security de-encryption.

Claim 10. (new) A tamper resistant processor system according to claim 9, wherein said chips possess an obscurant covering.

Claim 11. (new) A tamper resistant processor system according to claim 9, wherein said chips possess a self-destruct function.

Claim 12. (new) A tamper resistant processor system according to claim 11, wherein said self-destruct function destructs after first use.

Claim 13. (new) A tamper resistant processor system according to claim 2, wherein said encryption algorithm is randomly encrypted.

Claim 14. (new) A tamper resistant processor system according to claim 2, wherein de-encryption key and algorithm self-destruct after one use.